Multi party computation motivated by the birthday problem

Péter Hudoba, Péter Burcsi

Abstract:
The birthday problem is a widely known observation, can be found in most of the textbooks on probability. In this talk we are focusing on the following case of the problem: there are n people in a classroom and we want to decide if there are two people who were born on the same day of the year. During the decision making process, we want to keep all information secret.
We consider multiple ways to securely solve the decision problem and compare them by computational and communication aspects.

Keywords: secret multi-party computation, birthday problem, probability theory

Extended abstract

Birthday problem

One version of the birthday problem is described in [1, 2, 3] as the following: n people are selected at random. What is the probability that at least r people will have the same birthday. The widely known version is, the $n = 23$ and $r = 2$. The probability of the event that we will have two people who have been born on the same day is more than 50%.

Secure multi-party computation

Secure multi-party computation (MPC) is a field in cryptography, where the parties compute a function with their inputs jointly while keeping those inputs private. The problem in discussion, which we are focusing on is a special MPC problem. Read more in [4].

Some naive solutions

We can deduct the algorithm to the socialist millionaire problem, where we decide if the two participants have same number or not without geting any information about the other's number. If we ask all of the participants to decide if they have same birthday, we can solve the problem with $\frac{n(n-1)}{2}$ socialist millionaire solving. There are solutions for this MPC problem in [5],[6].

We can also deduct to a voting protocol. If we ask all of the participants to vote for every day, we can solve the problem in 365 voting rounds.

Security

What does "keep all information in secret" mean? Firstly, it means that at the end of the process no participant knows any other's birth date, but in this case that is also considered an information if an adversary knows that Alice and Bob have the same birthday.

This talk

In this talk we will explain multiple ways to solve the problem, show complexity and share implementations in Python.

References

[1] Frank H Mathis. A generalized birthday problem. *SIAM Review*, 33(2):265–270, 1991.

[2] David Wagner. A generalized birthday problem. In *Annual International Cryptology Conference*, pages 288–304. Springer, 2002.

[3] Morton Abramson and WOJ Moser. More birthday surprises. *The American Mathematical Monthly*, 77(8):856–858, 1970.

[4] Martin Hirt. *Multi Party Computation: Efficient Protocols, General Adversaries, and Voting*. Hartung-Gorre, 2001.

[5] Fabrice Boudot, Berry Schoenmakers, and Jacques Traore. A fair and efficient solution to the socialist millionaires problem. *Discrete Applied Mathematics*, 111(1-2):23–36, 2001.

[6] Hsiao-Ying Lin and Wen-Guey Tzeng. An efficient solution to the millionaires problem based on homomorphic encryption. In *International Conference on Applied Cryptography and Network Security*, pages 456–466. Springer, 2005.